Shavlik Patch for Microsoft System Center

User's Guide

For use with Microsoft System Center Configuration Manager 2012

Copyright

Copyright © 2014 Shavlik. All rights reserved. This product is protected by copyright and intellectual property laws in the United States and other countries as well as by international treaties.

No part of this document may be reproduced or retransmitted in any form or by any means electronic, mechanical, or otherwise, including photocopying and recording for any purpose other than the purchaser's personal use without written permission of Shavlik.

Trademarks

Shavlik is a trademark of Shavlik in the United States and other jurisdictions. Microsoft, Windows, and System Center Configuration Manager are either trademarks or registered trademarks of Microsoft Corporation.

All other trademarks, tradenames, or images mentioned herein belong to their respective owners.

Document Information and Print History

Document number: N/A

Date	Version	Description
February 2014	Initial version	Initial release of the **Shavlik Patch for Microsoft System Center User's Guide**.

Table of Contents

PREPARING TO USE SHAVLIK PATCH 5
Welcome 5
System Requirements 5
Installing the Shavlik Patch Configuration Manager Add-in 6
What the Shavlik Patch Add-in Adds to Configuration Manager 7
Understanding the Information in the Shavlik Patch Grid 8
Configuring Your Shavlik Patch Settings 9
WSUS Server Tab 9
WSUS Server Information 9
Code Signing Certificate Information 9
Account Tab 10
Schedule Tab 10
Using the Filters 11
Default Filters 11
Custom Filters 11
HOW TO PUBLISH UPDATES 13
Manually Publishing Third-Party Updates 13
Automatically Publishing Updates Using a Recurring Scheduled Task 16
Viewing and Managing Scheduled Publications 18
EXPIRING THIRD-PARTY UPDATES 19
SUPPORT INFORMATION 20
Supported Products 20
Technical Assistance 20
APPENDIX A : CREATING AND DISTRIBUTING CERTIFICATES 21
Overview 21
Reference 21
Certificate Requirements 21
Creating a Code Signing Certificate 22
Creating a Code Signing Certificate Using a CA 22
Using Shavlik Patch and WSUS to Create a Code Signing Certificate 22
Importing a Certificate 25
Export Certificate 26
Distributing the Certificate 27
Using Group Policy to Distribute the Certificate 27
Using MMC to Manually Distribute the Certificate 27

This page intentionally left blank.

The document is designed for duplex printing.

PREPARING TO USE SHAVLIK PATCH

Welcome

Welcome to Shavlik Patch for Microsoft System Center, an add-in that extends Microsoft's System Center Configuration Manager capabilities by enabling you to publish third-party updates and legacy products no longer supported by Configuration Manager. With Shavlik Patch you leverage a single Configuration Manager workflow for publishing updates for both Microsoft and non-Microsoft products.

Shavlik Patch consists of two components:

- **Update catalog:** Contains the detection and deployment logic used to patch non-Microsoft products and legacy Microsoft products. The catalog consists of a large number of update files from a number of different software vendors including Adobe, Apple, Firefox, Sun, and others.
- **Add-in to the Configuration Manager console:** Used to select updates from the catalog, publish them to your WSUS servers, and synchronize with Configuration Manager. This allows you to patch your legacy Microsoft products and your non-Microsoft products using the same Configuration Manager workflow used to patch Microsoft products.

System Requirements

Here are the requirements for installing and using Shavlik Patch:

- Shavlik Patch installs as an add-in to an existing Configuration Manager 2012 console (SP1 or later). The Configuration Manager console must be installed on one of these Windows operating systems:
  - Windows Server 2012 or later
  - Windows Server 2008 R2 SP1 or later
  - Windows 8 or later
  - Windows 7 SP1 or later
- .NET Framework 4.5 or later

  If you are missing this requirement, .NET Framework 4.5.1 will be installed for you during the installation of Shavlik Patch.
- Windows Server Update Services (WSUS) client requirements:
  - If Shavlik Patch is installed on the primary WSUS server and you are using Windows Server 2012 or Windows 8, then the WSUS API and the PowerShell cmdlets features must be enabled.
  - If WSUS is on a remote Windows 8 or Windows 8.1 machine, then the remote admin tools feature must be installed on that machine. The version of the remote admin tools and the version of WSUS must match or you will not be able to deploy updates.
  - If the primary WSUS server is running WSUS 3.0 SP2, then the WSUS 3.0 SP2 Administration Console must be installed on the same machine as Shavlik Patch. Patches KB2720211 and KB2734608 must be applied to both the WSUS server and the Configuration Manager Console machines.
- The Microsoft Task Scheduler service must be enabled and the user must have the rights necessary to create scheduled tasks.

- Shavlik Protect Cloud account
- The user running Shavlik Patch must be a member of the WSUS Administrators group on the WSUS server.
- Client machine requirements:

  Each of your client machines must meet the following requirements in order to deploy non-Microsoft updates distributed by a WSUS server:

  - Must contain a copy of the code signing certificate in the appropriate certificate stores
  - Must have enabled the **Allow signed updates from an intranet Microsoft update service location** policy setting

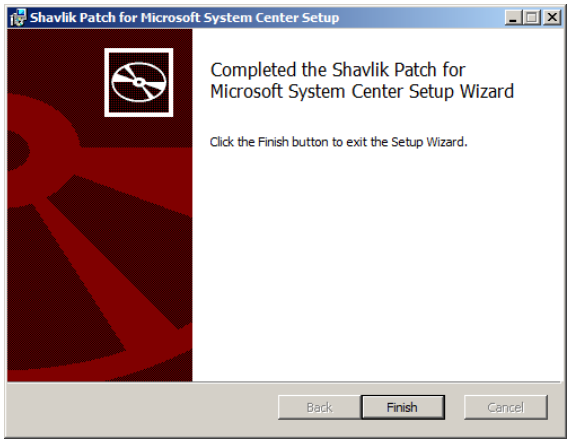
Installing the Shavlik Patch Configuration Manager Add-in

Note: You must be running as Administrator in order to install the add-in.

1. Using a Web browser, go to: www.shavlik.com/downloads/
2. Click the **Shavlik Patch** tab.
3. Download the **Shavlik Patch for Configuration Manager 2012** setup file.
4. Close System Center Configuration Manager.
5. Begin the Shavlik Patch installation by double-clicking the file named **SCCMPatchSetup.exe**.

   - If .NET Framework 4.5 or later is not installed on the Configuration Manager machine, you will be prompted to install .NET Framework 4.5.1 before continuing with the installation. Follow the on-screen instructions for installing this prerequisite.
   - If all prerequisites are installed, the license agreement is displayed. You must accept the terms of the license agreement in order to install the program.
6. Enable the check box to accept the license agreement and then click **Install**.

   After the files have been installed the **Completed** dialog is displayed.

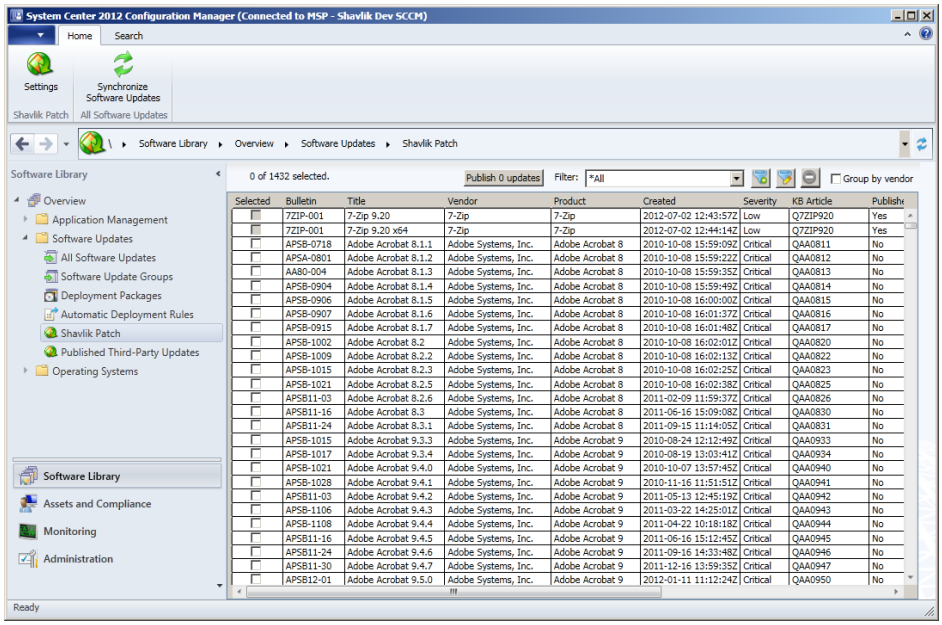

Shavlik Patch for Microsoft System Center Setup
Completed the Shavlik Patch for Microsoft System Center Setup Wizard
Click the Finish button to exit the Setup Wizard.
Back
Finish
Cancel

7. Click **Finish**.

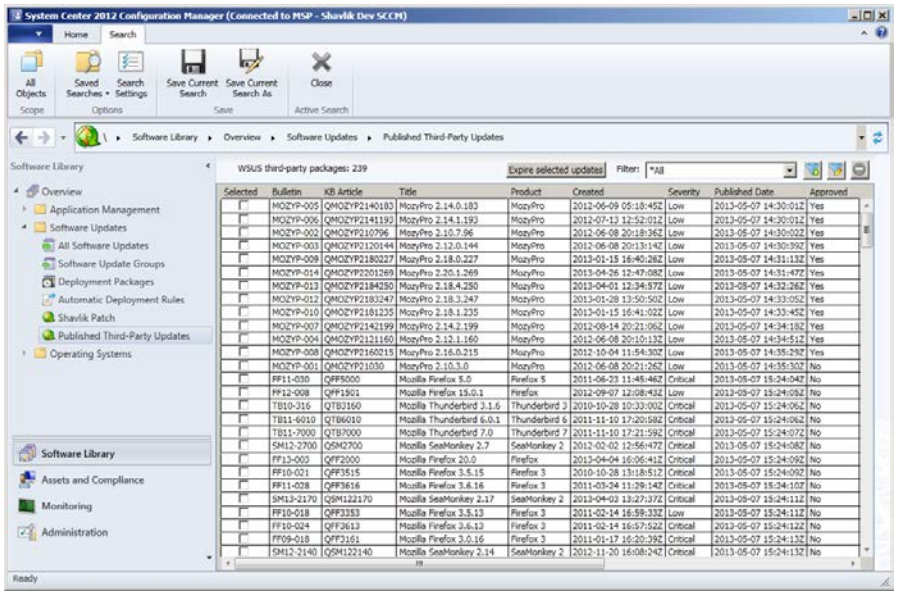
What the Shavlik Patch Add-in Adds to Configuration Manager

Installing the Shavlik Patch add-in will add two new list items to the **Software Library > Software Updates** folder. It will also add a **Settings** toolbar button to the Configuration Manager **Home** tab when either of the two new list items are selected.

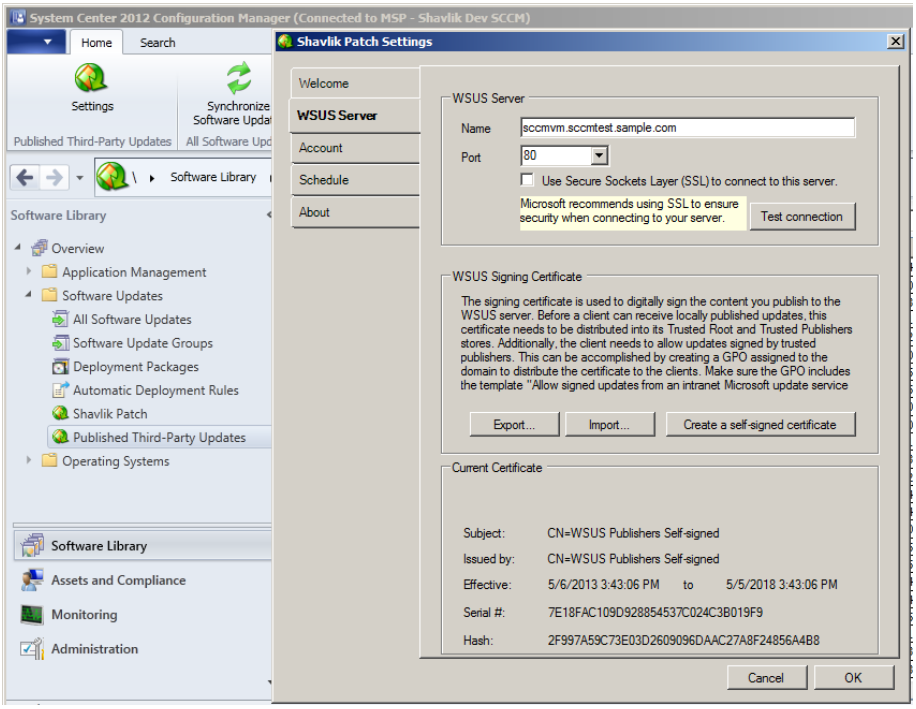
- **Shavlik Patch:** Contains all the updates available in the Shavlik Patch catalog. You will use this list to locate and publish updates.



- **Published Third-Party Updates:** Contains all the third-party updates that have been published to WSUS. The updates may have been published using Shavlik Patch or by another mechanism. You will use this list to review and manage the updates. The most common use will be to expire updates.



- **Settings:** This toolbar button is available on the **Home** tab when **Shavlik Patch** or **Published Third-Party Updates** is selected. You will use this button to set up local publishing, to enter your Shavlik Protect Cloud credentials, and to schedule recurring publication tasks.



Understanding the Information in the Shavlik Patch Grid

The **Shavlik Patch** grid contains a number of unique columns that help you identify the status of each update.

- **Published:** Indicates if the update has been published to WSUS.
- **Published Revision:** This number is incremented each time a revision to that update is published. All published updates will have a number greater than zero.
- **Revised:** Indicates if the update is a revision to an update that was previously published. If so, the check box in the **Selected** column will be enabled. Publishing such an update will create a new revision and will increment the **Published Revision** number.

  A revision update alters only the metadata and not the update package. A revision is posted to the Shavlik Patch catalog whenever any of the following need updating:

  - The detection logic that determines if a patch applies to a system and if it is already installed
  - Any text related to the update

Configuring Your Shavlik Patch Settings

The first time you use the Shavlik Patch add-in the **Shavlik Patch Settings** dialog will automatically be displayed. You must use this dialog to specify how to connect to your WSUS server and to your Protect Cloud account. You can return to this dialog at any time using the **Settings** button on the **Home** tab.

WSUS Server Tab

The **WSUS Server** tab is used to configure how the add-in will communicate with your WSUS Server. It is also used to define the certificate that will be used to digitally sign the content that is published to the WSUS server.

WSUS Server Information

- **Name:** Confirm the name or IP address of your WSUS Server. This information will normally be detected and automatically populated.
- **Port:** Confirm the port number used when making a connection to your WSUS Server. The default value for unsecured connections is either 80 or 8530. For secured connections you will typically use either 443 or 8531.
- **Secure Connection:** If your WSUS Server has been configured to use a secure connection, enable this check box. A secure connection is mandatory if you need to import a signing certificate. See *Importing a Certificate* in Appendix A for more information.
- **Test connection:** If you want to test your ability to access the WSUS Server, click **Test connection**.

Code Signing Certificate Information

A code signing certificate is required in order to publish updates to the WSUS server. If you already have a signing certificate in place it will be shown in the **Current Certificate** area.

You can perform the following certificate tasks:

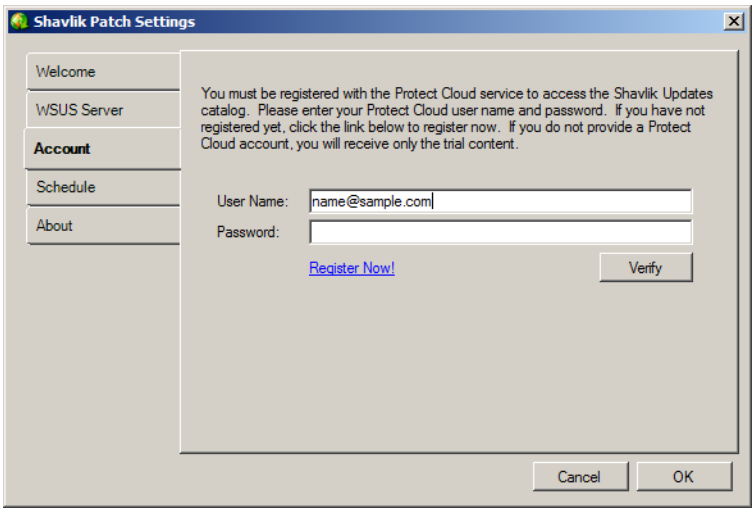
- **Export:** Exports the current certificate from within Shavlik Patch. After exporting the certificate you will distribute it to your clients and to your infrastructure machines (e.g. other machines that run the Shavlik Patch add-in, downstream WSUS servers, and Windows Update clients). This is necessary in order for the machines to receive locally published updates.
- **Import:** Imports a code signing certificate that was created by a Certificate Authority (CA). A secure connection is required in order to import a certificate.
- **Create a self-signed certificate:** Creates a code signing certificate for your enterprise. This process uses the services of WSUS to create the certificate.

For detailed information on exporting, importing, and creating certificates, see *Appendix A: Creating and Using Certificates*.

Account Tab

You must be signed in to the Shavlik Protect Cloud service in order for the add-in to automatically access and download the full Shavlik Patch catalog. The add-in uses your Protect Cloud account to periodically check for a new catalog. If you do not have a Protect Cloud account you will only receive trial content, which consists of only a few sample updates.

Note: For more information about the Shavlik Protect Cloud, go to: https://protectcloud.shavlik.com.


Shavlik Patch Settings
Welcome
WSUS Server
Account
Schedule
About
You must be registered with the Protect Cloud service to access the Shavlik Updates catalog. Please enter your Protect Cloud user name and password. If you have not registered yet, click the link below to register now. If you do not provide a Protect Cloud account, you will receive only the trial content.
User Name:
name@sample.com
Password:
Register Now!
Verify
Cancel
OK

- **User name:** Type the user name that you use to authenticate to your Protect Cloud account.
- **Password:** Type the password that you use to authenticate to your Protect Cloud account.
- **Register Now:** If you don't have a Protect Cloud account, click this button and follow the on-screen instructions to become a registered user. You must be a registered use in order to access the full Shavlik Patch catalog.
- **Verify:** If you want to test your ability to connect to your Protect Cloud account using the supplied credentials, click **Verify**. If you cannot connect to your account you will not be able to access the full Shavlik Patch catalog.

Schedule Tab

This tab is used to publish updates using a recurring scheduled task. For more information on this tab, see the section titled *Automatically Publishing Updates Using a Recurring Scheduled Task*.

Using the Filters

Information displayed in the **Shavlik Patch** list and the **Published Third-Party Updates** list can be filtered to search for specific updates. You can also use a filter when scheduling a recurring task.

Default Filters

The default filters are identified by a leading asterisk. Default filters cannot be modified or deleted. The default filters include the following:

Shavlik Patch List

- ***All:** All updates are displayed
- ***Not-Published:** Only the updates that have not been published to WSUS are displayed
- ***Published:** Only the updates that have been published to WSUS are displayed
- ***Selected:** Only the updates you select in the grid are displayed

Published Third-Party Updates List

- ***All:** All updates are displayed
- ***Selected:** Only the updates you select in the grid are displayed

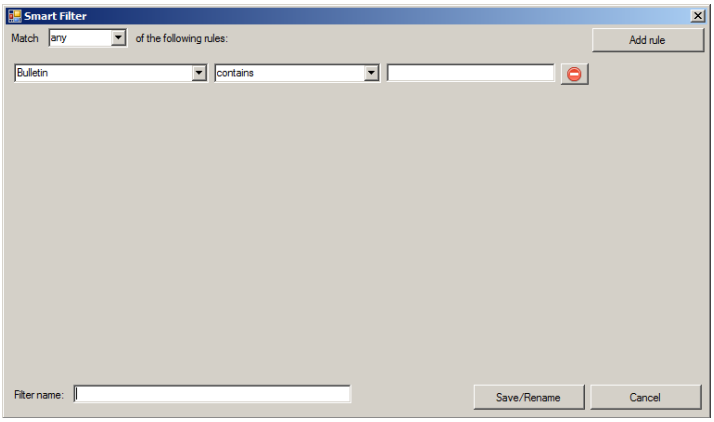
Custom Filters

You can create your own custom filters. This powerful tool enables you to specify exactly which updates are displayed. Each custom filter is comprised of one or more rules. You can define as many rules in a filter as needed.

To create a new filter:

1. Click the New Filter icon ( ).

   The **Filter** dialog is displayed.



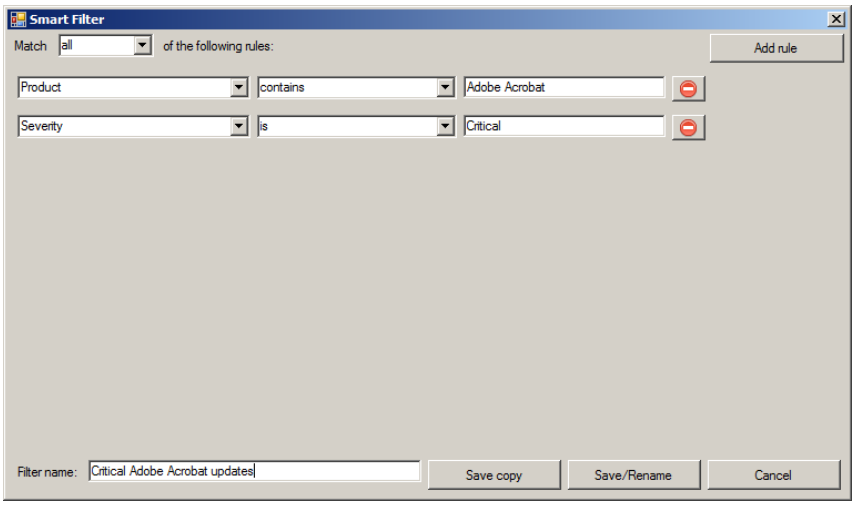
2. Specify which rules in the filter must be matched.
    - **All:** Only those updates that match all the rules in the filter will be displayed
    - **Any:** Updates that match at least one rule in the filter will be displayed
3. Define one or more rules.

    To define a rule, select an option in each of the first two logic boxes and then type the criteria in the third box. To add another rule simply click **Add rule**.

    Note: If you define a rule that does not make sense (for example: "Bulletin is less than 3") the rule will be ignored.
4. Type a name for the filter.
5. Click **Save/Rename**.

Example

Assume you want to see a list of all critical updates for Adobe Acrobat. You simply create the following filter:



HOW TO PUBLISH UPDATES

Manually Publishing Third-Party Updates

You can manually publish one or more third-party updates. The updates can be published immediately or be scheduled for publication at some point in the future. The Microsoft Task Scheduler is used to schedule the publication. The publication always runs as a separate task, but can be monitored while it is running.

1. Within the Configuration Manager **Software Library** workspace, expand the **Software Updates** folder and click on **Shavlik Patch**.

2. Enable the **Selected** check box for each update that you want to publish.

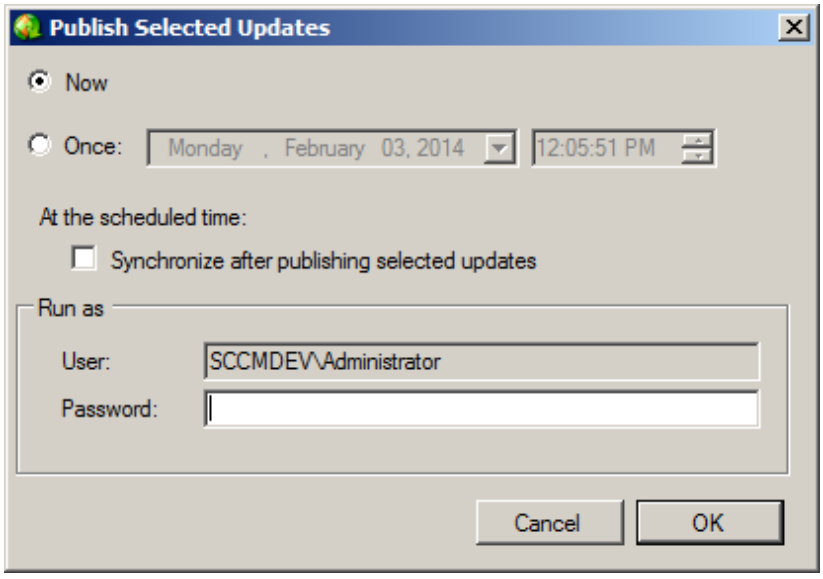
   The **Selected** check box will be disabled if the latest revision of the update has already been published or has recently been scheduled for publication.

   To locate the desired updates you can:

   - Use a filter
   - Use the **Group by vendor** check box
   - Sort the columns by clicking in the column headers

3. Click **Publish # updates** (where # = the number of selected updates).

   The **Publish Selected Updates** dialog is displayed.



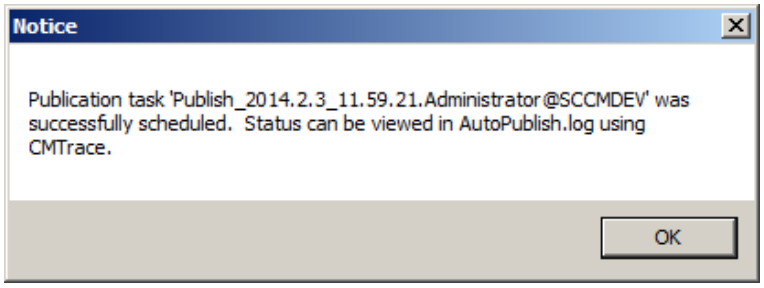
4. Specify when and how you want to publish the update(s).

   - **Now:** The publishing process will begin as soon as you click **OK**.
   - **Once:** Schedule the publication process to occur at some time in the future.

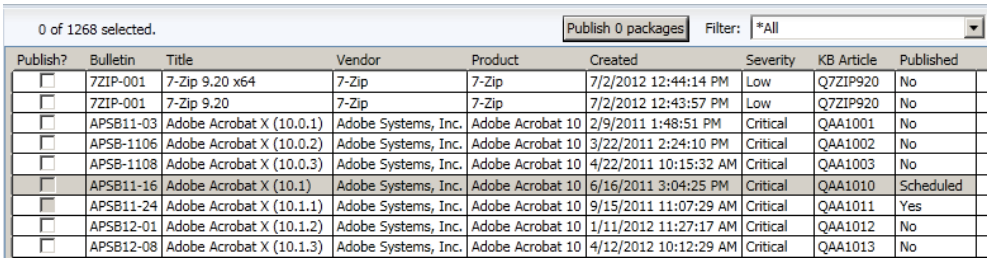
- **Synchronize after publishing selected updates:** If you want Configuration Manager to automatically synchronize itself with the WSUS database as part of this task, enable this check box. This will cause an incremental synchronization to be performed. If you do not enable this check box, the published update(s) will not be available until your regularly scheduled synchronization process occurs.
- **Run as:** Provide the credentials needed to add the publishing task to Microsoft Scheduler.

5. Click **OK**.

   The **Notice** dialog is displayed.


Notice
Publication task 'Publish_2014.2.3_11.59.21.Administrator@SCCMDEV' was successfully scheduled. Status can be viewed in AutoPublish.log using CMTrace.
OK

6. During the publication process the **Published** column status will show **Scheduled**.

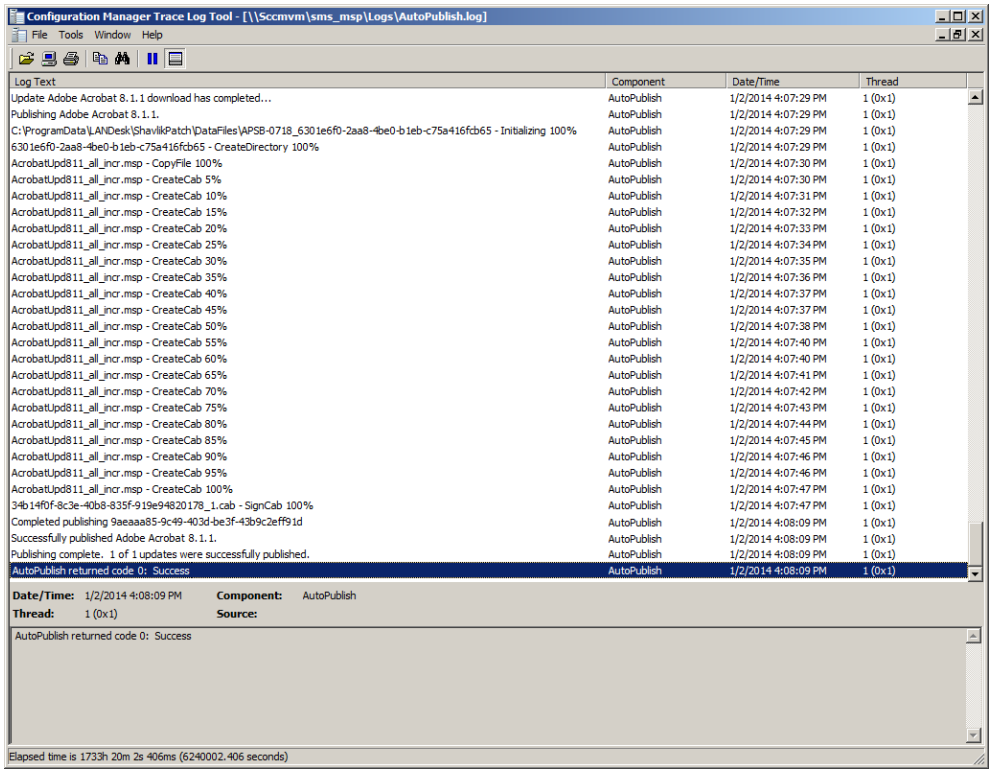


Publish?	Bulletin	Title	Vendor	Product	Created	Severity	KB Article	Published
☐	7ZIP-001	7-Zip 9.20 x64	7-Zip	7-Zip	7/2/2012 12:44:14 PM	Low	Q7ZIP920	No
☐	7ZIP-001	7-Zip 9.20	7-Zip	7-Zip	7/2/2012 12:43:57 PM	Low	Q7ZIP920	No
☐	APSB11-03	Adobe Acrobat X (10.0.1)	Adobe Systems, Inc.	Adobe Acrobat 10	2/9/2011 1:48:51 PM	Critical	QAA1001	No
☐	APSB-1106	Adobe Acrobat X (10.0.2)	Adobe Systems, Inc.	Adobe Acrobat 10	3/22/2011 2:24:10 PM	Critical	QAA1002	No
☐	APSB-1108	Adobe Acrobat X (10.0.3)	Adobe Systems, Inc.	Adobe Acrobat 10	4/22/2011 10:15:32 AM	Critical	QAA1003	No
☐	APSB11-16	Adobe Acrobat X (10.1)	Adobe Systems, Inc.	Adobe Acrobat 10	6/16/2011 3:04:25 PM	Critical	QAA1010	Scheduled
☐	APSB11-24	Adobe Acrobat X (10.1.1)	Adobe Systems, Inc.	Adobe Acrobat 10	9/15/2011 11:07:29 AM	Critical	QAA1011	Yes
☐	APSB12-01	Adobe Acrobat X (10.1.2)	Adobe Systems, Inc.	Adobe Acrobat 10	1/11/2012 11:27:17 AM	Critical	QAA1012	No
☐	APSB12-08	Adobe Acrobat X (10.1.3)	Adobe Systems, Inc.	Adobe Acrobat 10	4/12/2012 10:12:29 AM	Critical	QAA1013	No

7. (Optional) Use the Configuration Manager Trace Log Tool to open the AutoPublish.log file and monitor the publication process.

   AutoPublish.log is written by all one-time or recurring scheduled jobs that publish to WSUS.

Here is an example of the AutoPublish.log file:


Configuration Manager Trace Log Tool - [\\Sccmvm\sms_msp\Logs\AutoPublish.log]
File Tools Window Help
Log Text | Component | Date/Time | Thread
Update Adobe Acrobat 8.1.1 download has completed... AutoPublish 1/2/2014 4:07:29 PM 1 (0x1)
Publishing Adobe Acrobat 8.1.1. AutoPublish 1/2/2014 4:07:29 PM 1 (0x1)
C:\ProgramData\LANDesk\ShavlikPatch\DataFiles\APSB-0718_6301e6f0-2aa8-4be0-b1eb-c75a416fcb65 - Initializing 100% AutoPublish 1/2/2014 4:07:29 PM 1 (0x1)
6301e6f0-2aa8-4be0-b1eb-c75a416fcb65 - CreateDirectory 100% AutoPublish 1/2/2014 4:07:29 PM 1 (0x1)
AcrobatUpd811_all_incr.msp - CopyFile 100% AutoPublish 1/2/2014 4:07:30 PM 1 (0x1)
AcrobatUpd811_all_incr.msp - CreateCab 5% AutoPublish 1/2/2014 4:07:30 PM 1 (0x1)
AcrobatUpd811_all_incr.msp - CreateCab 10% AutoPublish 1/2/2014 4:07:31 PM 1 (0x1)
AcrobatUpd811_all_incr.msp - CreateCab 15% AutoPublish 1/2/2014 4:07:32 PM 1 (0x1)
AcrobatUpd811_all_incr.msp - CreateCab 20% AutoPublish 1/2/2014 4:07:33 PM 1 (0x1)
AcrobatUpd811_all_incr.msp - CreateCab 25% AutoPublish 1/2/2014 4:07:34 PM 1 (0x1)
AcrobatUpd811_all_incr.msp - CreateCab 30% AutoPublish 1/2/2014 4:07:35 PM 1 (0x1)
AcrobatUpd811_all_incr.msp - CreateCab 35% AutoPublish 1/2/2014 4:07:36 PM 1 (0x1)
AcrobatUpd811_all_incr.msp - CreateCab 40% AutoPublish 1/2/2014 4:07:37 PM 1 (0x1)
AcrobatUpd811_all_incr.msp - CreateCab 45% AutoPublish 1/2/2014 4:07:37 PM 1 (0x1)
AcrobatUpd811_all_incr.msp - CreateCab 50% AutoPublish 1/2/2014 4:07:38 PM 1 (0x1)
AcrobatUpd811_all_incr.msp - CreateCab 55% AutoPublish 1/2/2014 4:07:40 PM 1 (0x1)
AcrobatUpd811_all_incr.msp - CreateCab 60% AutoPublish 1/2/2014 4:07:40 PM 1 (0x1)
AcrobatUpd811_all_incr.msp - CreateCab 65% AutoPublish 1/2/2014 4:07:41 PM 1 (0x1)
AcrobatUpd811_all_incr.msp - CreateCab 70% AutoPublish 1/2/2014 4:07:42 PM 1 (0x1)
AcrobatUpd811_all_incr.msp - CreateCab 75% AutoPublish 1/2/2014 4:07:43 PM 1 (0x1)
AcrobatUpd811_all_incr.msp - CreateCab 80% AutoPublish 1/2/2014 4:07:44 PM 1 (0x1)
AcrobatUpd811_all_incr.msp - CreateCab 85% AutoPublish 1/2/2014 4:07:45 PM 1 (0x1)
AcrobatUpd811_all_incr.msp - CreateCab 90% AutoPublish 1/2/2014 4:07:46 PM 1 (0x1)
AcrobatUpd811_all_incr.msp - CreateCab 95% AutoPublish 1/2/2014 4:07:46 PM 1 (0x1)
AcrobatUpd811_all_incr.msp - CreateCab 100% AutoPublish 1/2/2014 4:07:47 PM 1 (0x1)
34b14f0f-8c3e-40b8-835f-919e94820178_1.cab - SignCab 100% AutoPublish 1/2/2014 4:07:47 PM 1 (0x1)
Completed publishing 9aeaaa85-9c49-403d-be3f-43b9c2eff91d AutoPublish 1/2/2014 4:08:09 PM 1 (0x1)
Successfully published Adobe Acrobat 8.1.1. AutoPublish 1/2/2014 4:08:09 PM 1 (0x1)
Publishing complete. 1 of 1 updates were successfully published. AutoPublish 1/2/2014 4:08:09 PM 1 (0x1)
AutoPublish returned code 0: Success AutoPublish 1/2/2014 4:08:09 PM 1 (0x1)
Date/Time: 1/2/2014 4:08:09 PM Component: AutoPublish
Thread: 1 (0x1) Source:
AutoPublish returned code 0: Success
Elapsed time is 1733h 20m 2s 406ms (6240002.406 seconds)

8. When the update is successfully published the **Published** column status will change to **Yes** the next time the grid is refreshed.

   Note that the check box in the **Selected** column will be disabled if the latest revision of an update has been published.

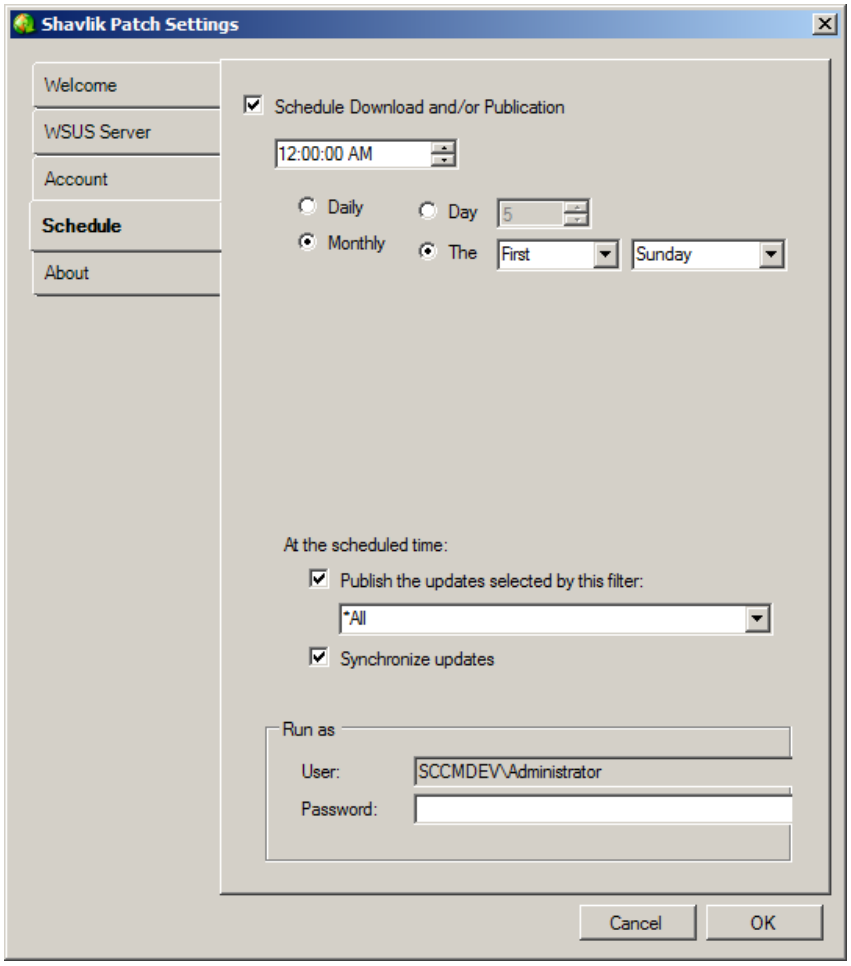
   You can sort the **Published** column to see the list of updates that have been published, or you can use the ***Published** filter.

Automatically Publishing Updates Using a Recurring Scheduled Task

You can automatically publish updates on a recurring basis by creating a scheduled task. You can only schedule one recurring task.

1. Within the Configuration Manager **Software Library** workspace, expand the **Software Updates** folder and click on **Shavlik Patch**.
2. On the **Home** tab, click **Settings** (or right-click Shavlik Patch and click **Settings**).

   The **Shavlik Patch Settings** dialog is displayed.



3. On the **Schedule** tab, specify when the scheduled task should run and what action(s) should occur.

   - **Schedule Download and/or Publication:** Specify when you want the recurring task to run.
   - **Publish the packages selected by this filter:** Enables you to specify which updates you want to publish on a recurring basis. You can choose either the predefined filter named ***All** (meaning all unpublished updates in the Shavlik Patch catalog) or any of your custom filters.

Example 1: To publish all updates that have not been previously published, select the ***All** filter. This is an easy way to automatically publish new updates on a recurring basis.

Example 2: Assume you have previously created a custom filter that identifies all unpublished critical updates for the products you use in your organization. Simply select that filter here to publish just those updates on a recurring basis.

- **Synchronize updates:** If you want Configuration Manager to automatically synchronize itself with the WSUS database as part of this task, enable this check box. This will cause an incremental synchronization to be performed. If you do not enable this check box, the published updates will not be available until your regularly scheduled synchronization process occurs.
- **Run as:** Provide the credentials needed to add the publishing task to Microsoft Scheduler.

4. (Optional) Use the Configuration Manager Trace Log Tool to open the AutoPublish.log file and monitor the publication process.

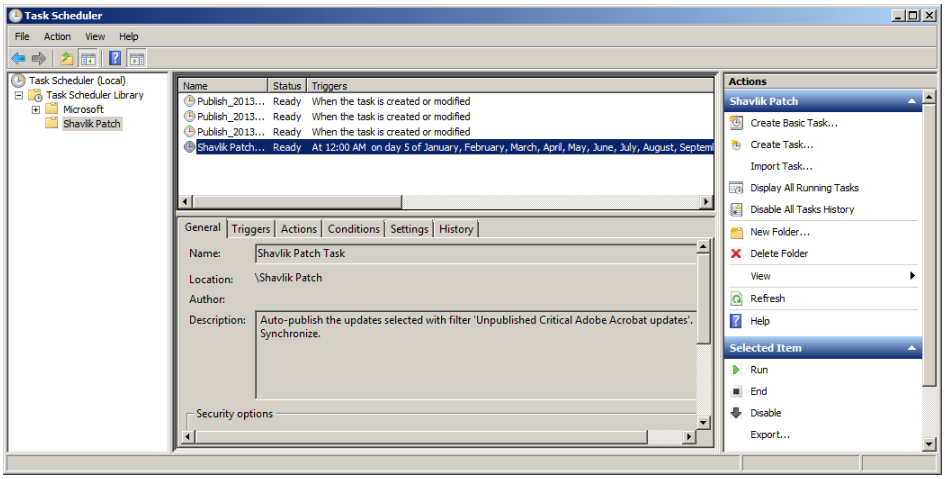
   The AutoPublish.log file is written by any one-time or recurring scheduled jobs that publish to WSUS.

You can use the Auto-Publish feature of Shavlik Patch in conjunction with Automatic Deployment rules in Configuration Manager to keep clients up to date with the latest third-party updates.

Viewing and Managing Scheduled Publications

You can use the Microsoft Task Scheduler to view and manage your scheduled publications. To access Shavlik Patch scheduled tasks, select **Start > Administrator Tools > Task Scheduler > Task Scheduler Library > Shavlik Patch**.

- One-time tasks can be run, deleted, disabled, or rescheduled using the Microsoft Task Scheduler.



- If you alter a recurring auto-publish schedule using the Shavlik Patch **Settings** dialog, the task will be automatically rescheduled.
- If you clear the **Schedule download and /or publication** check box in the **Settings** dialog and click **OK**, the recurring task will be deleted from the Microsoft Task Scheduler.
- After a publishing task completes, the task will continue to be displayed in the Microsoft Task Scheduler for one to two days.

EXPIRING THIRD-PARTY UPDATES

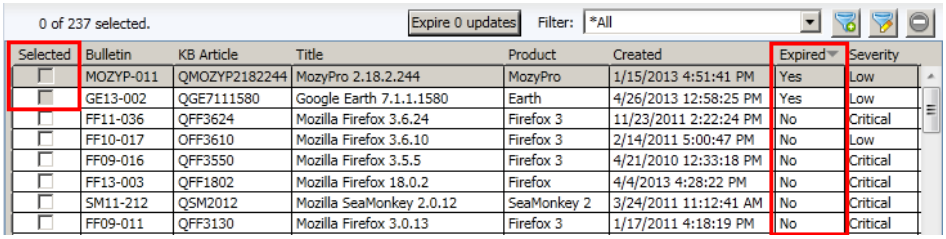
You can expire third-party updates that have been invalidated by the product vendor or that have been superseded by other updates. Expired software updates cannot be deployed. The updates you set as expired can then be deleted using the WSUS cleanup tool.

To expire an update:

1. Within the Configuration Manager **Software Library** workspace, expand the **Software Updates** folder and click on **Published Third-Party Updates.**
2. Select the updates that you want to expire.
3. Click **Expire # updates** (where # = the number of selected updates).

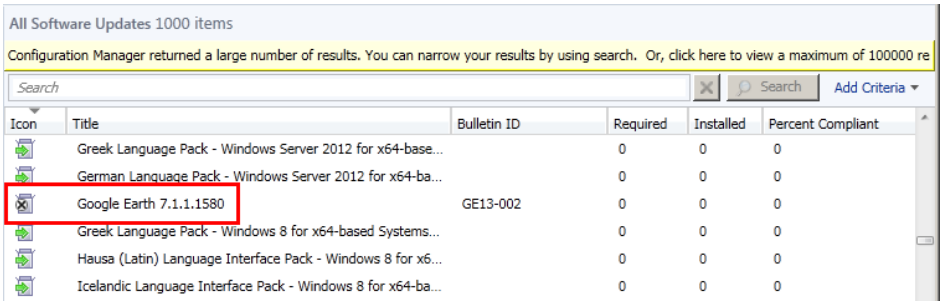
To view expired updates:

- Within the **Published Third-Party Updates** list, sort the list using the **Expired** column. Note that the check boxes in the **Selected** column will be disabled. For example:



Selected	Bulletin	KB Article	Title	Product	Created	Expired	Severity
☐	MOZYP-011	QMOZYP2182244	MozyPro 2.18.2.244	MozyPro	1/15/2013 4:51:41 PM	Yes	Low
☐	GE13-002	QGE7111580	Google Earth 7.1.1.1580	Earth	4/26/2013 12:58:25 PM	Yes	Low
☐	FF11-036	QFF3624	Mozilla Firefox 3.6.24	Firefox 3	11/23/2011 2:22:24 PM	No	Critical
☐	FF10-017	QFF3610	Mozilla Firefox 3.6.10	Firefox 3	2/14/2011 5:00:47 PM	No	Low
☐	FF09-016	QFF3550	Mozilla Firefox 3.5.5	Firefox 3	4/21/2010 12:33:18 PM	No	Critical
☐	FF13-003	QFF1802	Mozilla Firefox 18.0.2	Firefox	4/4/2013 4:28:22 PM	No	Critical
☐	SM11-212	QSM2012	Mozilla SeaMonkey 2.0.12	SeaMonkey 2	3/24/2011 11:12:41 AM	No	Critical
☐	FF09-011	QFF3130	Mozilla Firefox 3.0.13	Firefox 3	1/17/2011 4:18:19 PM	No	Critical

- Within the **All Software Updates** list, expired updates are represented by the expired icon ( ). For example:


All Software Updates 1000 items
Configuration Manager returned a large number of results. You can narrow your results by using search. Or, click here to view a maximum of 100000 re
Search
Search
Add Criteria

Icon	Title	Bulletin ID	Required	Installed	Percent Compliant
	Greek Language Pack - Windows Server 2012 for x64-base...		0	0	0
	German Language Pack - Windows Server 2012 for x64-ba...		0	0	0
	Google Earth 7.1.1.1580	GE13-002	0	0	0
	Greek Language Pack - Windows 8 for x64-based Systems...		0	0	0
	Hausa (Latin) Language Interface Pack - Windows 8 for x6...		0	0	0
	Icelandic Language Interface Pack - Windows 8 for x64-ba...		0	0	0

SUPPORT INFORMATION

Supported Products

For a complete list of the products supported by Shavlik Patch, see:

http://community.shavlik.com/docs/DOC-2285

Technical Assistance

For technical assistance with Shavlik Patch, please refer to one of the following support options:

- Browse the Shavlik Patch section of the Shavlik community page at: http://community.shavlik.com. You will need to become a member of the community in order to gain full access to all available resources.
- Open a support request at http://support.shavlik.com/CaseLogging.aspx
- Phone Technical Support at (866) 407-5279
- View online video tutorials at www.shavlik.com/support/training-videos/patch

APPENDIX A : CREATING AND DISTRIBUTING CERTIFICATES

Overview

A code signing certificate is required when using Shavlik Patch with Configuration Manager and WSUS to publish third-party updates. In general, you must:

1. Create a code signing certificate.

   You can do this using either an internal Certificate Authority (CA) or your WSUS server.

2. (Conditional) If you use an internal CA to create the code signing certificate, you must import the certificate into WSUS, which you can do using Shavlik Patch.

   If you use WSUS to create the code signing certificate, the certificate will be automatically imported into WSUS.

3. Export the certificate.

4. Distribute the code signing certificate to the appropriate certificate stores on all your WSUS servers and to your client machines.

   - Trusted Publishers certificate store
   - Trusted Root Certificate Authorities certificate store

This appendix provides details on how to accomplish each of these tasks.

Reference

For detailed certificate information beyond that presented in this appendix, please see the following articles.

- For information on establishing a trust relationship to support third-party patching:

  http://msdn.microsoft.com/en-us/library/bb902479(v=vs.85).aspx

- For information on why WSUS in Windows Server 2012 R2 no longer by default supports generating code signing certificates, and for a workaround:

  http://blogs.technet.com/b/wsus/archive/2013/08/15/wsus-no-longer-issues-self-signed-certificates.aspx

  Note: Shavlik Patch will automatically invoke this workaround if you choose to create a self-signed certificate using the **Settings** dialog.

Certificate Requirements

The minimum requirements of the signing certificate are:

- The private key must be exportable
- The key size must be 2048 or greater
- It must be a code-signing certificate

Creating a Code Signing Certificate

Note: You can skip this section if you already have a code signing certificate.

You have two options for creating a code signing certificate:

- Use a code signing certificate that is created using an internal CA
- Use the Shavlik Patch user interface to have WSUS create a self-signed code signing certificate

Creating a Code Signing Certificate Using a CA

Creating a certificate from a trusted CA offers a couple of advantages:

- Distribution: Eliminates the need to distribute the certificate to other machines in the same domain.
- Management: Simplifies management because the certificate can be managed the same way as other certificates in your environment.

Follow your normal process for creating a certificate from your internal CA. After you have created the certificate you must write it to the WSUS server. You can do this using the **Import Certificate** feature in Shavlik Patch. See the section titled *Importing a Certificate* for more details.

Using Shavlik Patch and WSUS to Create a Code Signing Certificate

Using the Shavlik Patch interface, you can instruct WSUS to create a self-signed code signing certificate for your enterprise. Creating a code signing certificate is enabled by default on WSUS prior to Windows Server 2012 R2.

Important! If you are using WSUS on Windows Server 2012 R2, the ability to create self-signed code signing certificates has been deprecated and is disabled by default. You can, however, restore this capability by using the workaround described in this article:

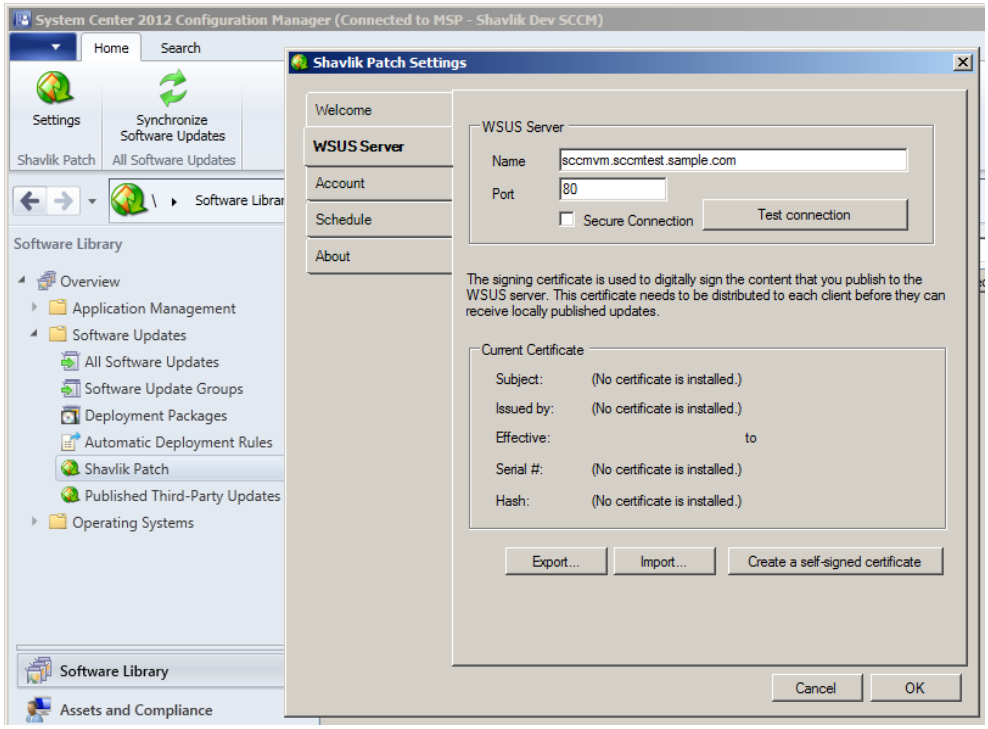
http://blogs.technet.com/b/wsus/archive/2013/08/15/wsus-no-longer-issues-self-signed-certificates.aspx

If you chose to create a code signing certificate in Shavlik Patch using a Software Update Point (WSUS server) on Windows Server 2012 R2 or later, this workaround will be applied automatically.

To create a self-signed code signing certificate using WSUS:

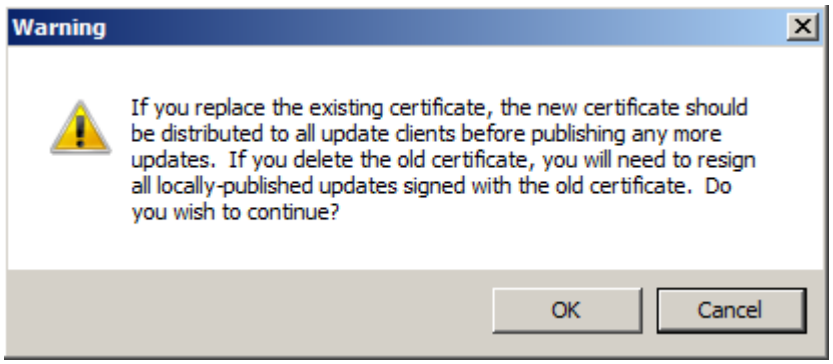
1. Within the Configuration Manager **Software Library** workspace, expand the **Software Updates** folder and click on **Shavlik Patch**.
2. On the Configuration Manager **Home** tab, click **Settings**.

3. On the **Shavlik Patch Settings** dialog, select the **WSUS Server** tab.



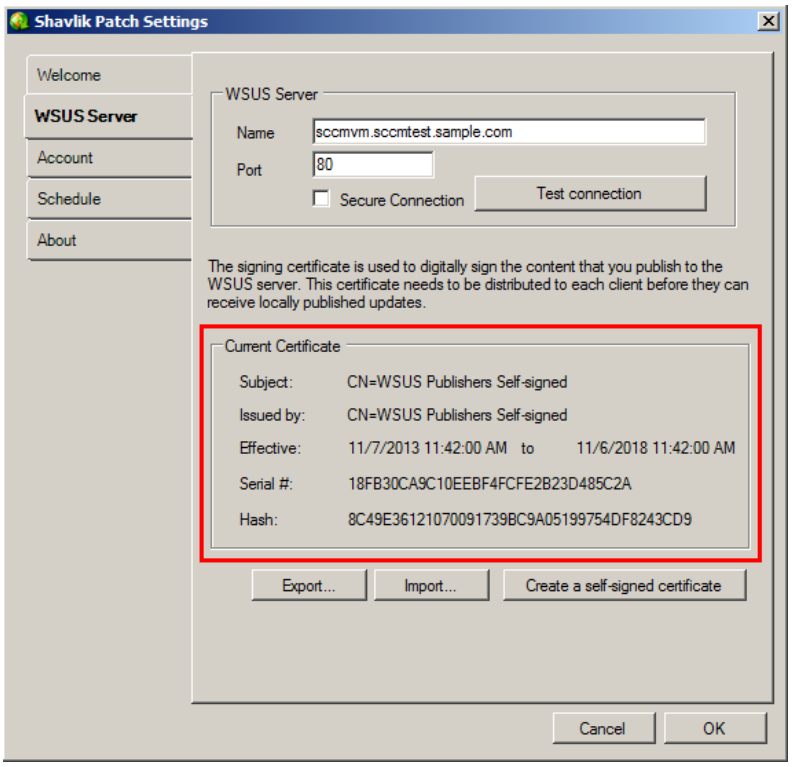
4. Click **Create a self-signed certificate**.

   If a certificate already exists the following **Warning** dialog is displayed:


Warning
If you replace the existing certificate, the new certificate should be distributed to all update clients before publishing any more updates. If you delete the old certificate, you will need to resign all locally-published updates signed with the old certificate. Do you wish to continue?
OK
Cancel

   Do not proceed unless you are certain you need a different certificate. The warning message explains what you will need to do if you are replacing or deleting an existing certificate.

The new certificate is created on the WSUS server and is registered with WSUS. Details of the certificate are displayed in the **Current Certificate** area. For example:



The certificate is also installed in the following certificate stores on the local Configuration Manager console:

- Trusted Root Certification Authorities
- Trusted Publishers

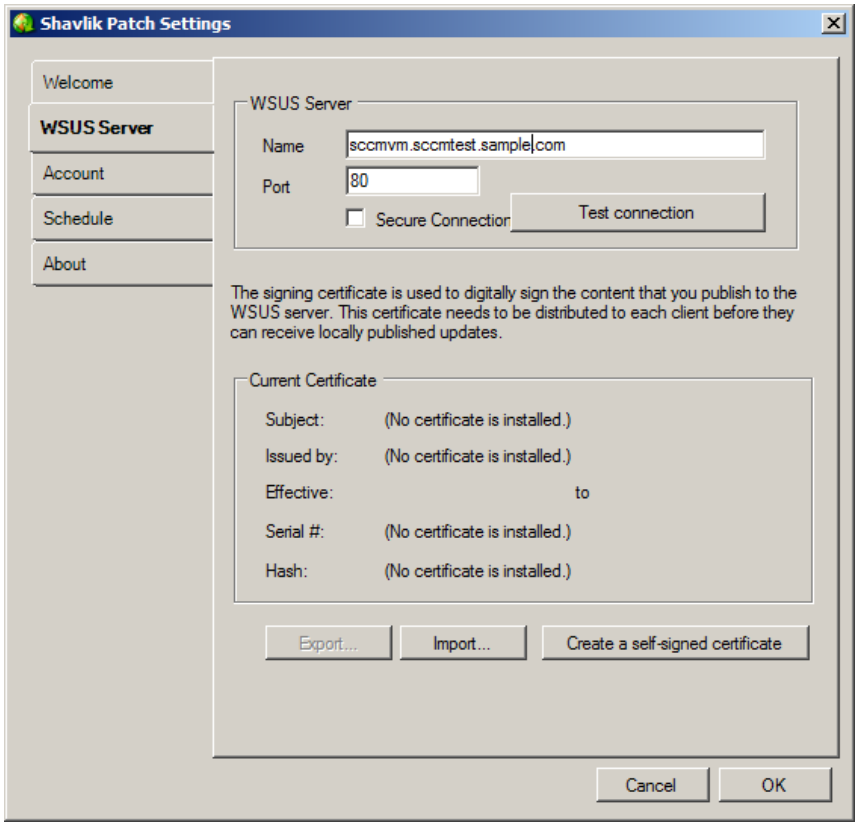
Importing a Certificate

This section applies only if you created your code signing certificate using an internal CA. Importing the certificate will write the certificate to the WSUS Server and to the appropriate certificate stores on your machine. You do not need to use the import process if you used WSUS to create a code signing certificate, as that certificate was automatically written to the proper locations.

Note: In order to import a certificate you must have a secure (SSL) connection to the WSUS server. This is accomplished in part by enabling the **Secure Connection** check box in the **WSUS Server** area of the **WSUS Server** tab. You must also configure your IIS to use SSL.

To import a certificate:

1. Within the Configuration Manager **Software Library** workspace, expand the **Software Updates** folder and click on **Shavlik Patch**.
2. On the Configuration Manager **Home** tab, click **Settings**.
3. On the **Shavlik Patch Settings** dialog, select the **WSUS Server** tab.



4. Click **Import**.
5. Navigate to the certificate file and click **OK**.

Export Certificate

The export process is used to export the certificate used to sign the published updates to an accessible location on your network.

Note: The export process will only export the public certificate; the private key is NOT exported.

1. Within the Configuration Manager **Software Library** workspace, expand the **Software Updates** folder and click on **Shavlik Patch**.
2. On the Configuration Manager **Home** tab, click **Settings**.
3. On the **Shavlik Patch Settings** dialog, select the **WSUS Server** tab.
4. Click **Export**.
5. Specify the location and file name and then click **Save**.

After exporting the certificate, you will need to distribute it to any other WSUS servers and to your client machines. This is necessary in order for the machines to receive locally published updates.

The distribution process is described in the next section.

Distributing the Certificate

You must distribute the code-signing certificate to all servers that house your Configuration Manager and WSUS consoles and to all of your client machines. Which certificate store(s) the certificate is copied to depends on how the code-signing certificate was created.

- If your code signing certificate was created by WSUS (and is therefore a self-signed code signing certificate), you will need to copy the certificate to the following locations on all your WSUS servers and to your client machines:
    - Trusted Publishers certificate store
    - Trusted Root Certificate Authorities certificate store
- If the code-signing certificate was issued by a CA whose root is already trusted by your clients, you only need to copy the certificate to the Trusted Publishers certificate store on your WSUS and client machines.

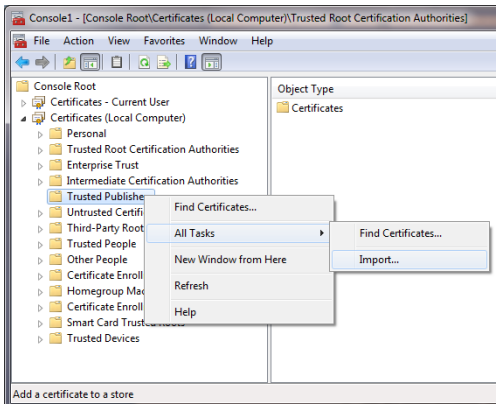
Using Group Policy to Distribute the Certificate

A common method for distributing the code-signing certificate to your servers and/or client machines is to use Group Policy. For general instructions on how to perform this task, see Step 3 in this article:
http://blogs.technet.com/b/jasonlewis/archive/2011/07/12/system-center-updates-publisher-signing-certificate-requirements-amp-step-by-step-guide.aspx

Using MMC to Manually Distribute the Certificate

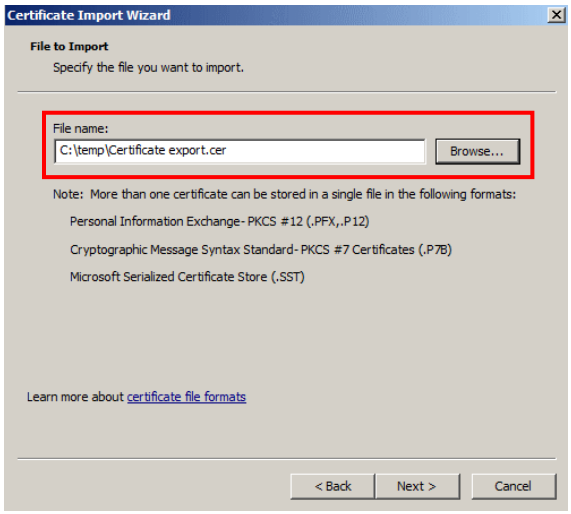
Another method for distributing the code-signing certificate is to use MMC. This is an easy method for distributing the certificate to a handful of local machines but might prove impractical for distributing the certificate to many machines spread across your organization.

1. On the target machine, start Microsoft Management Console (MMC).
2. In the Certificates store, right-click **Trusted Publishers** and select **All Tasks > Import**.

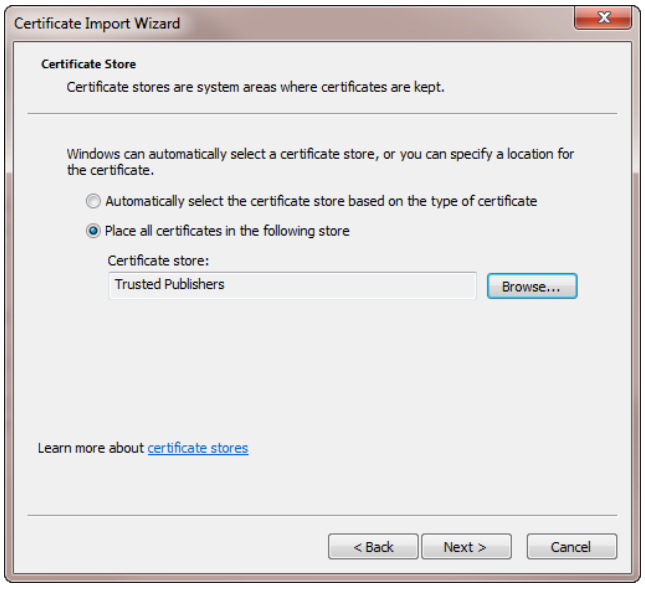


3. On the **Welcome to the Certificate Import Wizard** dialog, click **Next**.

4. On the **File to Import** dialog, browse for your public key file and then click **Next**.


Certificate Import Wizard
File to Import
Specify the file you want to import.
File name:
C:\temp\Certificate export.cer
Browse...
Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)
Learn more about certificate file formats
< Back
Next >
Cancel

5. On the **Certificate Store** dialog, choose **Place all certificates in the following store** and then click **Next**.


Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Trusted Publishers
Browse...
Learn more about certificate stores
< Back
Next >
Cancel

6. On the **Completing the Certificate Import Wizard dialog**, click **Finish**.

7. On the confirmation dialog click **OK**.

8. (Conditional) If you created your certificate using WSUS, repeat Steps 2 – 7, only this time select **Trusted Root Certification Authorities** in Step 2.